Single Connect Kron

Datasheet

TWO-FACTOR AUTHENTICATION MANAGER (2FA)

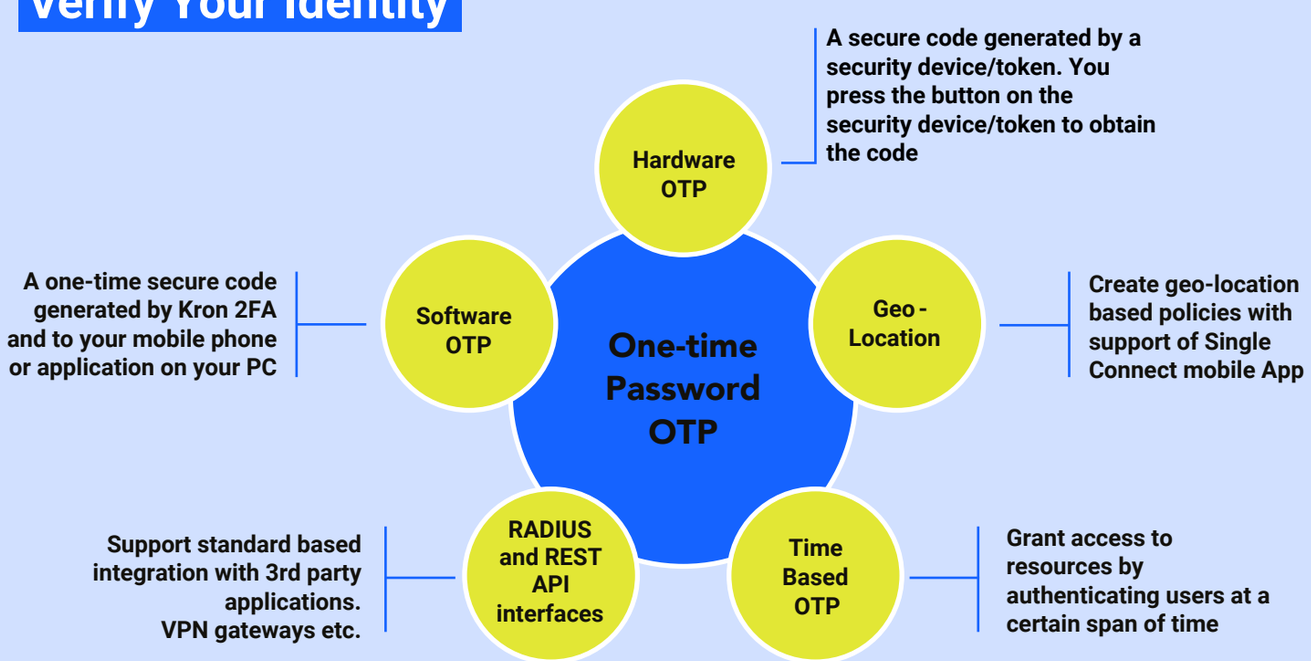
Enhance Your Authentication Process

There are thousands of different types of accounts in an enterprise infrastructure; personal accounts (of employees, contractors, etc.), local administrative accounts, privileged user accounts, domain administrative accounts, emergency accounts, service accounts, application accounts. **You may train your employees on cyber security and take many technical preventive actions, but accounts are still (and will continue to be) hacked/leaked/compromised.**

For example, socially engineered malware and phishing attacks are the most common **attack types** and there is nothing much you can do other than training employees, but they will still accidentally be victims of such attacks. Whatever preventive actions you take, you must have a plan B to prevent **compromised** accounts/identities from accessing critical data/assets of the enterprise.

While accessing to critical systems during the authentication process, Single Connect 2FA combines **two different authentication factors** to complete the login process and to achieve a greater level of security: User credentials and a secure code (token) generated by Single Connect 2FA Manager, Single Connect Mobile App or a Hardware Token.

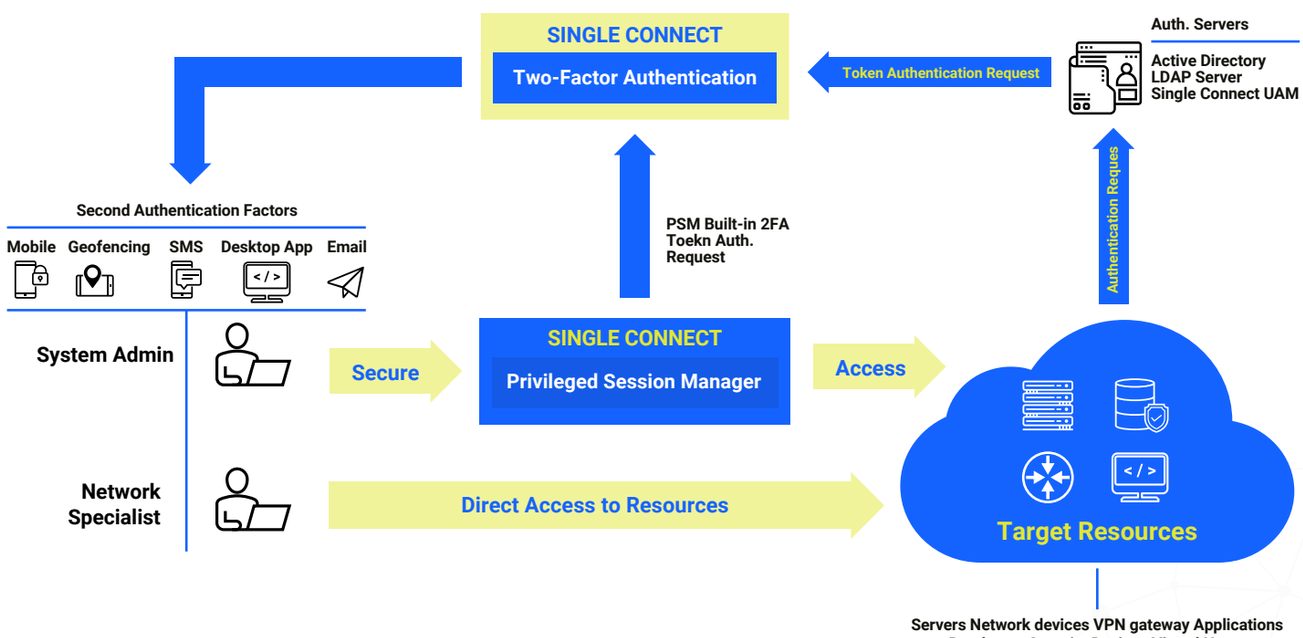
Second Layer of Security to Verify Your Identity



Single Connect Kron

Datasheet

HOW 2FA MANAGER WORKS



Step 1: The user connects to the target host directly or via Single Connect PSM and enters username & password.

Step 2: The target host check the user credentials with defined authentication server. Authentication server asks for a second authentication through Single Connect 2FA.

Step 3: Single Connect 2FA Manager generates a secure code (token) (one-time use only), and then either sends the token to the user (via SMS/email/mobile app) or the user generates the same token offline on its mobile app.

Step 4: User enters the secure code (The secure codes are generally reset every 30 seconds).

Step 5: Target host sends the token to Single Connect 2FA Manager.

Step 6: Single Connect 2FA Manager checks whether the received token is correct or not; if yes, access is granted.

Single Connect Kron

Datasheet

FEATURES & BENEFITS

Two-factor authentication enables to strengthen the protection of vital resources by drastically reducing the chances of various security attacks including identity theft, phishing, online fraud and more. Even if an employee's account is compromised, it is still not possible to access the enterprise's critical assets/resources, unless the employee's mobile phone (or email account) is stolen as well.

2FA Manager provides another level of security, even if the password is weak or **non-expiry**.

Single Connect 2FA Manager **provides** you with broad authentication methods and features, granting customers to define different type of use cases, **security levels**, and attack vectors. 2FA Manager supports both online (SMS, Email and Single Connect Mobile App) and offline (Single Connect Mobile App and hard token) token authentication.

Single Connect 2FA Manager supports hardware-based authentication which is a technique for user authentication that relies on a dedicated physical device (**such as a token**) held by an authorized user, in addition to a basic password, to grant access to critical resources. In hardware-based authentication method, these devices produce a unique secure code for a limited time to get access. The combination of the secure code and the password constitute a two-factor authentication system.

Single Connect 2FA Manager comprises another type of two-factor authentication method called **out-of-band** authentication. In this method, authentication process requires a secondary verification through a secure code delivered over an independent communication tunnel (SMS or e-mail) in addition to user credentials.

Single Connect 2FA Manager also supports software-based authentication that enables users to access the secure code of secondary **verification process through** a software application on the user's computer, smartphone, or mobile device.

Password sharing becomes irrelevant because any passwords shared with colleagues are useless by leveraging the **Single Connect 2FA** solution.

Auto lock user account when an employee terminates employment (integration with enterprise Active Directory or LDAP is required).

2FA Manager enables **geo-location** and time restrictions for secure access.

Single Connect 2FA Manager also enables two-factor authentication for external apps. Provides standard-based integration with RADIUS and **REST API** interfaces with external applications (VPNs, firewalls, email servers and others).

2FA Manager **pre-integrated** with other Single Connect modules.